HQMC
ISC BRIEF

FEBRUARY 6, 2007

Purpose

- To provide section ISCs with information and guidance pertaining to the status of the network, the future of the network and some recommended best practices to use while working on the network.

Agenda

- 0900-0915 PDS update/New CAC card/New watch (Capt Heslin)
- 0915-0925 SIPRNet way ahead (Maj Eiben)
- 0925-0945 Classified information spill procedures (GySgt Hodges)
- 0945-1005 Share drive class (Sgt Shaffer)
- 1005-1025 NMCI Issues (Mr. Benson)
- 1025-1030 Closing remarks and Q&A (Capt Heslin)

ARI OPERATIONS

- PDS Update
  - Timeline
  - New SIPRNet Requirements
- New CAC cards
  - Active card v5.4 vs. v6
    - Open trouble ticket with NMCI to install new software
    - Call the IT center for 7 day CLO exemption
- New IT Center watch
- SIPRNet way ahead (Maj Eiben)
  - New architecture

QUESTIONS?

SPILL PROCEDURES

INFORMATION ASSURANCE CHIEF

GySgt Hodges

SPILLAGE RESPONSIBILITIES

- <u>SCI's Responsibilities</u>
  - Reporting the incident to HQMC ARI
  - Gathering information
    1. Classification of spillage
    2. Which network is affected.
    3. Originator of the spillage
       A. Name, rank
       B. Command
       C. Phone number
       D. Email address

SPILLAGE RESPONSIBILITIES

3. Disconnect machines from the network
4. Rank, names, email addresses, phone #’s and office room #’s of all users affected.
5. Machine name and location of all machines infected.
6. Whether or not the material can be declassified.

SPILLAGE RESPONSIBILITIES

HQMC ARI INFORMATION ASSURANCE SECTION

- Receive notification from ISC
- Contact MCNOSC
- Contact NMCI and supply them with the spillage questionnaire
- Track trouble ticket until cleanup is completed
- Assist NMCI as needed.

NMCI SPILLAGE QUESTIONNAIRE 1 OF 3

1) Who is the Command IAM/IAM (Formally ISSM)?
Command: HQMC

Name: GS-14 Katzberg A.A.

Phone: 703.693.2138

2) Is this Unauthorized Disclosure on the Legacy/AOR'd systems, NMCI or both? If legacy, then User/IAM must contact the legacy help desk and provide information. If spillage occurred on NMCI or AOR Legacy, continue with the following steps.

3) When did the disclosure occur?

4) Did your command originate this disclosure?

5) Has the originator been contacted?

6) What is the Classification of the data spilled? (Confidential, Secret, Top Secret, U-NNPI, or C-NNPI)
(If data is Secret or below, open unclassified ticket. If message classification is above Secret, C-NNPI, Special Category (SPECAT) or above, then escalate the disclosure reporting to the High-Side Help Desk.)

NMCI SPILLAGE QUESTIONNAIRE 2 OF3

7) What is the Classification of the system data went to?

8) Was the disclosure material clearly marked?

9) Are there any special markings?

10) How many users are affected? Who did this get sent too? (Caller must provide either a list of valid user LOG ON names/Commands/ or valid NMCI distribution list. Check Global Address List (GAL) to verify distribution.)

11) Was a public folder involved?

12) What is the EXACT Subject Line of disclosure? (Regardless of the type of disclosure, get the caller to cut and paste sender, receiver, and subject line for you to place in ticket)

13) Is this disclosure?

a. Physical Media disclosure or Contamination?
b. E-mail?
c. Message traffic?

14) Physical Media disclosure or Contamination: (Hard drive, Floppy, Web page, Zip, etc)? (Media is contaminated when it contacts media of a higher classification)

a) What type of media was contaminated?
b) What are the names of the assets affected (workstation names, printer names, server names, etc)?
c) Has the IAM taken the affected workstations off the network?

NMCI SPILLAGE

QUESTIONNAIRE 3 0F3

15) E-mail disclosure. (One user sends classified E-mail or attachment to another user)
Was the disclosure contained within the E-mail or within an attachment?

Attachment:

16) Message disclosure.
What is the Date/Time/Group and originator of message:

17) Have you notified anyone else of this Disclosure? Did command IAM initiate SITREP?
Yes:
Who:

18) Have caller contact their Site Manager and Base Ops Manager with ticket number provided after this call.

QUESTIONS?

Contact Information

GySgt Kenneth Hodges
INFORMATION ASSURANCE CHIEF
703.693.2138
571.435.1374
KENNETH.HODGES@USMC.MIL

LEGACY NIPR FILE MIGRATION/ HOW TO MAP A NETWORK DRIVE

Sgt GARY SHAFFER

WHO WILL THIS IMPACT?

- **ALL HQMC USERS THAT USE THE ‘X’ DRIVE**
- **ANY INFORMATION LOCATED ON THE FOLLOWING FILE SERVERS**
  - **HQFS001**
  - **HQFS002**
  - **HQFS003**
  - **HQFS401**
  - **HQFS402**
  - **HQFS403_**

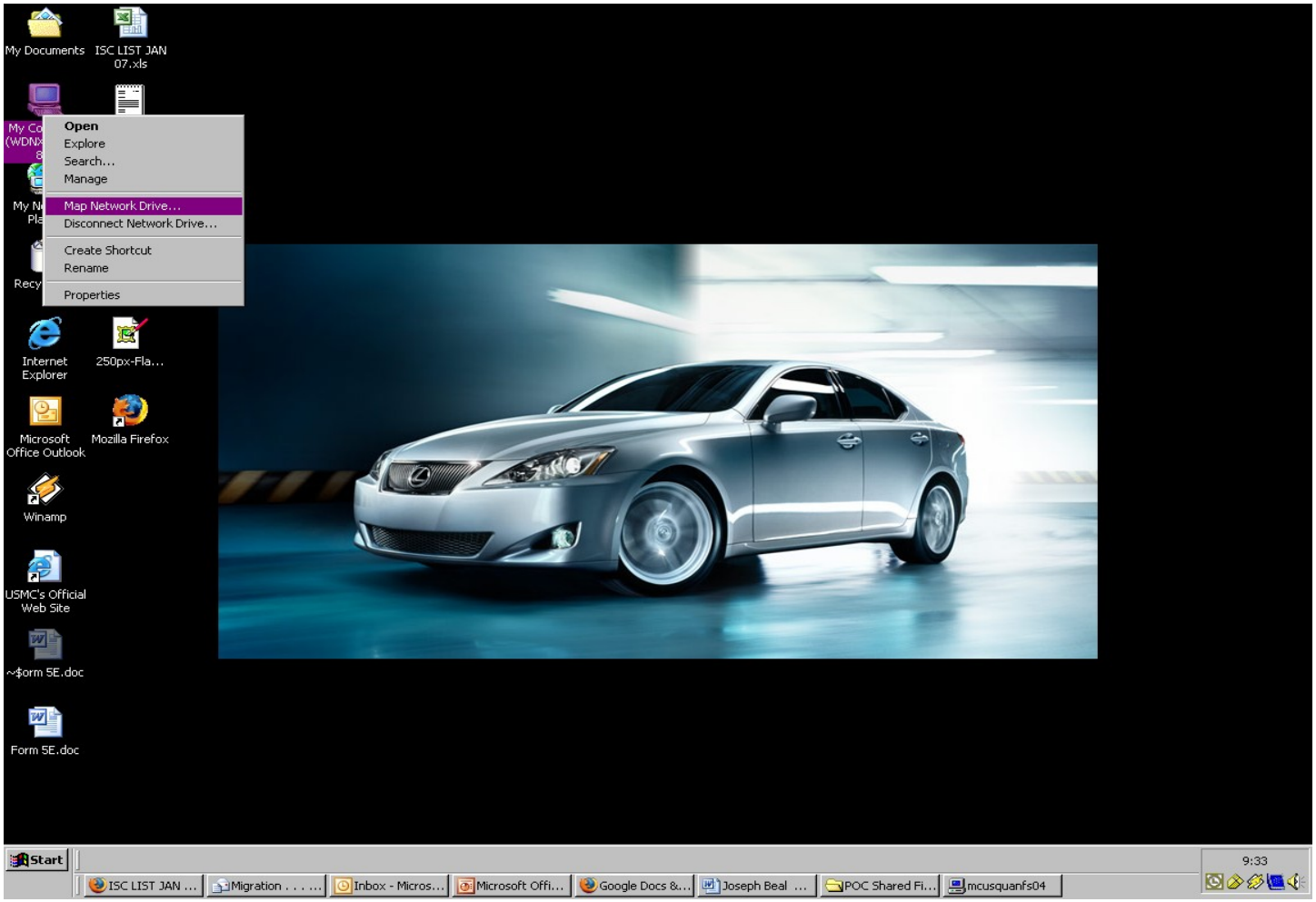
WHEN AND WHERE?

- SCHEDULE WILL BE DISTRIBUTED VIA E-MAIL
- HQMC IT CENTER OR AT YOUR RESPECTIVE SECTIONS

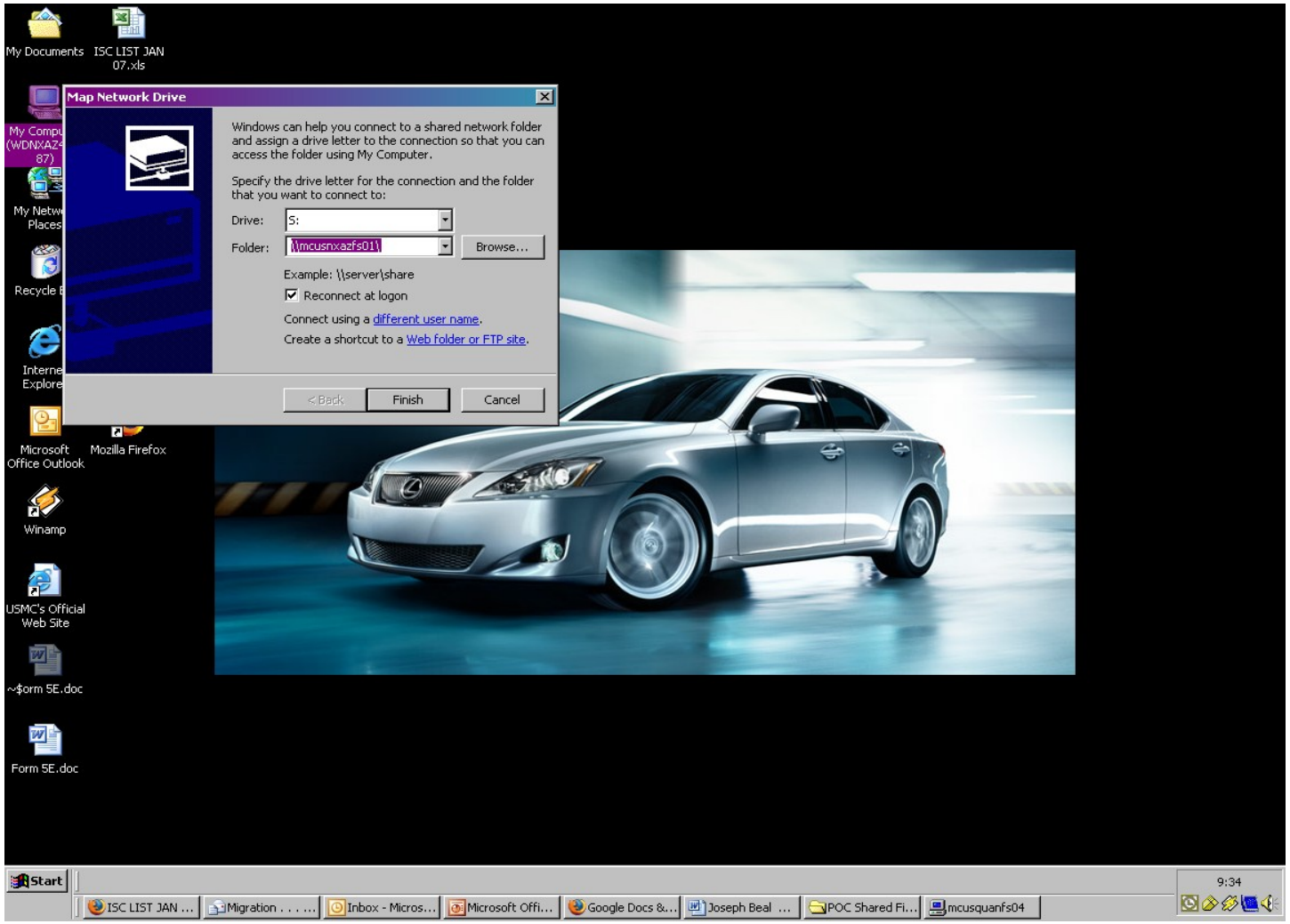
WHAT I NEED FROM YOU?

- **ISC PERMISSIONS**
  - Do you have them?
- **FOLDER ARCHITECTURE**
  - Make sure the folders are set up the way your section needs them
  - Access to folders will be set with the use of Security Groups
  - **USERS MUST CLEAN OUT THEIR FOLDERS!!!!!!!!**
    - **IF THEY DON'T NEED IT DELETE IT!**
- **SECURITY GROUPS**
  - Submit a MAC request to add or delete Security Groups
  - Keep Security Groups up-to-date.
- ****Mapping is based on OU membership****

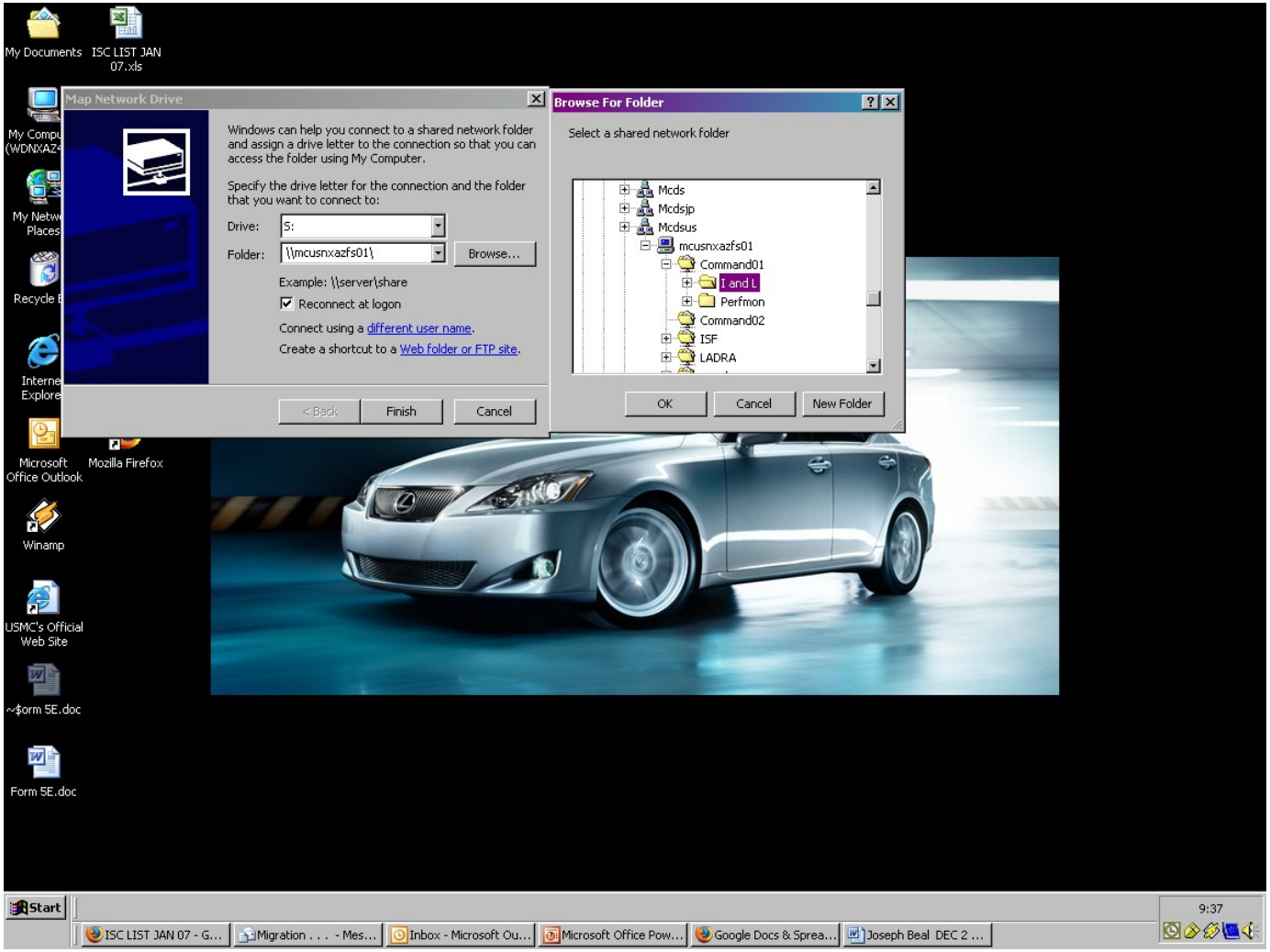
HOW TO MAP A NETWORK DRIVE



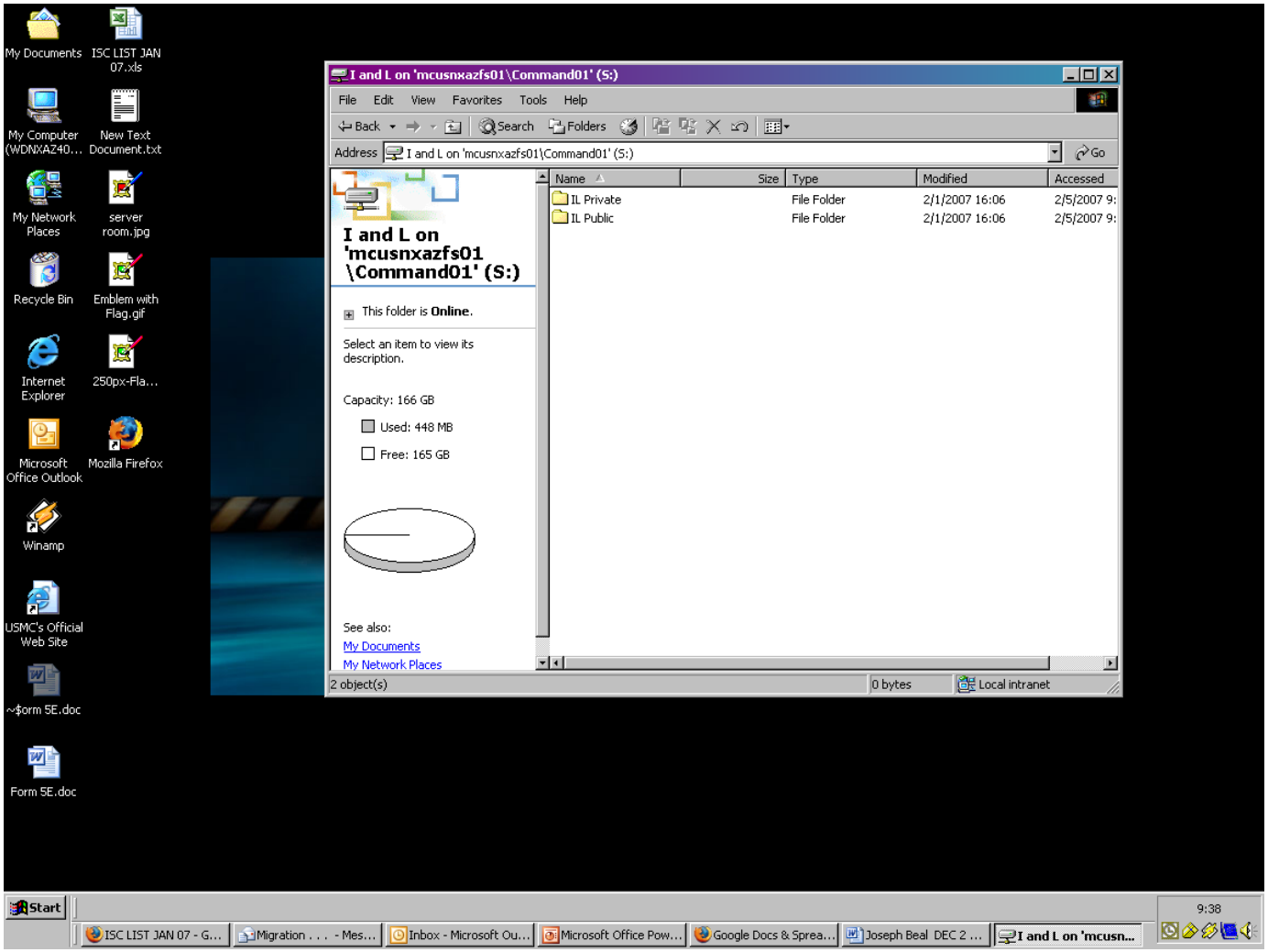
HOW TO MAP A NETWORK DRIVE (CONT.)



HOW TO MAP A NETWORK DRIVE (CONT.)



HOW TO MAP A NETWORK DRIVE (CONT.)



QUESTIONS?

Contact Information

Sgt Gary Shaffer

Legacy Migration NCOIC

703.693.1721

GARY.SHAFFER@USMC.MIL

NMCI Issues

Mr. Stewart Benson

NMCI Issues

- SEAT ORDERS
- BLACKBERRY RECONCILIATION
- BLACKBERRY/PRINTERS/OTHER ITEMS
- COMPUTER AND PRINTER DROPS
- WIRELESS CARDS
- CLIN 47 SOFTWARE CERTIFICATION
- FUNDING: NOW AND FOREVER

QUESTIONS?

Contact Information

Mr. Stewart Benson

Lead CTR, NCR

703-614-2109

STEWART.BENSON@USMC.MIL

Q&A

Contact Information

Capt Brian Heslin

ARI Operations Officer

703-614-4878

571-435-1399

brian.heslin@usmc.mil